AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listing of claims in the above-referenced application.

Listing of Claims:

1. (Currently Amended) A method of detecting computer viruses, comprising:

providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments;

an antivirus unit, that uses a particular operating system, scanning at least part of the disk space for viruses, wherein the part of the disk space that is scanned by the antivirus unit includes at least some parts of the first and second segments; [[and]]

the antivirus unit accessing non-native files created using operating systems different from the particular operating system that is used by the antivirus unit in connection with scanning at least parts of the disk space for viruses, wherein said antivirus unit scans at least one of the segments without using file-based information of the particular operating system or of any host having access to said at least one segment;

detecting write operations to tracks of the storage device; and

performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed.

2. (Original) A method, according to claim 1, wherein said first and second segments correspond to different physical portions of the disk space.

3. (Original) A method, according to claim 2, wherein said first and second segments overlap.

4. (Original) A method, according to claim 2, wherein the first and second segments do not overlap.

5. (Original) A method, according to claim 1, wherein the first and second segments correspond to logical entities.

6. (Original) A method, according to claim 5, wherein said first and second segments overlap.

7. (Original) A method, according to claim 5, wherein the first and second segments do not overlap.

8. -12. (Canceled)

13. (Original) A method, according to claim 1, further comprising:

implementing at least part of the antivirus unit using stand alone hardware.

14. (Original) A method, according to claim 1, further comprising:

implementing at least part of the antivirus unit as a process running on at least one of the hosts.

15. (Original) A method, according to claim 1, wherein useable areas of the disk space are partitioned into separate segments.

16. (Original) A method, according to claim 1, wherein the antivirus unit scans useable areas of the disk space.

17. (Canceled)

18. (Original) A method, according to claim 1, wherein a particular segment assigned to a first host is inaccessible to other hosts.

19. (Original) A method, according to claim 18, wherein all of the segments are at least readable by the antivirus unit.

20. (Original) A method, according to claim 1, wherein at least a portion of the antivirus unit is provided on at least some controllers for disks corresponding to the disk space.

21. (Canceled)

22. (Currently Amended) A method of scanning a storage device for viruses, comprising:

performing a first virus scan at a first time; and

performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system, wherein, when performing a virus scan accessing at least one part of the storage device that is also accessible to at least one host, scanning of said at least one part is performed without using file-based information of the particular operating system or of any host having access to said at least one part, and

wherein at least one of said performing said first virus scan and said performing said second virus scan includes:

detecting write operations to tracks of the storage device; and

performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed.

23. -25. (Cancelled)

26. (Previously Presented) A computer program product for detecting computer viruses, comprising:

means for accessing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments;

means that uses a particular operating system for scanning at least part of the disk space for viruses, wherein the part of the disk space that is scanned includes at least some parts of the first and second segments; and

means for accessing non-native files created using operating systems different from the particular operating system that is used in connection with scanning at least parts of the disk space for viruses, wherein, when performing a virus scan accessing at least one of the segments that is also accessible to at least one of said plurality of hosts, scanning of said at least one segment is performed without using file-based information of the particular operating system or of any host having access to said at least one segment.

27. (Original) A computer program product, according to claim 26, wherein said first and second segments correspond to different physical portions of the disk space.

28. (Original) A computer program product, according to claim 27, wherein said first and second segments overlap.

29. (Original) A computer program product, according to claim 27, wherein the first and second segments do not overlap.

30. (Original) A computer program product, according to claim 26, wherein the first and second segments correspond to logical entities.

31.-35. (Cancelled)

36. (Currently Amended) A computer program product for scanning a storage device for viruses, comprising:

means for performing a first virus scan at a first time; and

means for performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system, wherein, when performing a virus scan accessing at least one part of the storage device that is also accessible to at least one host, scanning of said at least one part is performed without using file-based information of the particular operating system or of any host having access to said at least one part, wherein at least one of said means for performing said first virus scan and said means for performing said second virus scan include:

means for detecting write operations to tracks of the storage device; and

means for performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed.

37.-38 (Canceled)

39. (Previously Presented) An antivirus scanning unit, comprising:

means for coupling to at least one storage device having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments;

means for using a particular operating system for scanning at least part of the at least one storage device for viruses, wherein the part that is scanned includes at least some parts of the first and second segments; and

means for accessing non-native files created using operating systems different from the particular operating system that is used in connection with scanning at least parts of the disk space for viruses, wherein, when performing a virus scan accessing at least one of the segments that is also accessible to at least one of said plurality of hosts, scanning of the at least one segment is performed without using file-based information of the particular operating system or of any host having access to said at least one segment.

40. (Original) An antivirus unit, according to claim 39, wherein said means for coupling includes means for coupling to only one storage device.

41. (Original) An antivirus unit, according to claim 39, wherein said means for coupling includes means for coupling to more than one storage device.

42. (Original) An antivirus unit, according to claim 39, further comprising:

means for coupling to at least one host.

43. (Original) An antivirus unit, according to claim 42, wherein said antivirus unit is interposed between said at least one storage device and said at least one host.

44. (Original) An antivirus unit, according to claim 42, wherein said antivirus unit is implemented as a process running on the at least one host.

45. (Original) An antivirus unit, according to claim 39, wherein said antivirus unit is implemented using stand alone hardware.

46. (Original) An antivirus unit, according to claim 39, wherein at least a portion of the antivirus unit is provided on at least some controllers for the at least one storage device.

47. (Currently Amended) An antivirus unit, comprising:

means for performing a first virus scan at a first time; and

means for performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system, wherein, when performing a virus scan accessing at least one part of the storage device that is also accessible to at least one host, scanning of said at least one part is performed without using file-based information of the particular operating system or of any host having access to said at least one part;

wherein at least one of said means for performing said first virus scan and said means for performing said second virus scan includes:

means for detecting write operations to tracks of the storage device; and

means for performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed.

48. (Canceled)

49. (Original) An antivirus unit, according to claim 47, wherein said antivirus unit is implemented using stand alone hardware.

50. (Original) An antivirus unit, according to claim 47, wherein at least a portion of the antivirus unit is provided on at least some controllers for the at least one storage device.

51. (Canceled)

52. (Previously Presented) The method of Claim 1, wherein the antivirus unit and a first of said plurality of hosts have access to a same segment and access to said same segment by said first host is denied when said same segment is being accessed by said antivirus unit.

53. (Previously Presented) The method of Claim 1, wherein the antivirus unit and a first of said plurality of hosts have access to a same segment and the antivirus unit is allowed to perform virus scanning on said same segment while said same segment is being accessed by said first host.

54. (Currently Amended) [[The method of Claim 1]] A method of detecting computer viruses, comprising:

providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments;

an antivirus unit, that uses a particular operating system, scanning at least part of the disk space for viruses, wherein the part of the disk space that is scanned by the antivirus unit includes at least some parts of the first and second segments; and

the antivirus unit accessing non-native files created using operating systems different from the particular operating system that is used by the antivirus unit in connection with scanning at least parts of the disk space for viruses, wherein said antivirus unit scans at least one of the segments without using file-based information of the particular operating system or of any

host having access to said at least one segment, wherein the antivirus unit accesses a portion of said disk space using a logical disk unit, a cylinder number and a track number, and the method further comprising:

detecting write operations to tracks of the device; and

performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed.

55. (Previously Presented) The computer program product of Claim 26, wherein said means for accessing non-native files and a first of said plurality of hosts have access to a same segment and access to said same segment by said first host is denied when said same segment is being accessed by said means for accessing non-native files.

56. (Previously Presented) The computer program product of Claim 26, wherein said means for accessing non-native files and a first of said plurality of hosts have access to a same segment and said means for accessing non-native files is allowed to perform virus scanning on said same segment while said same segment is being accessed by said first host.

57. (Previously Presented) The computer program product of Claim 26, wherein said means for accessing non-native files accesses a portion of said disk space using a logical disk unit, a cylinder number and a track number, and the computer program product further comprising:

means for detecting write operations to tracks of the device; and

means for performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed.

58. (Previously Presented) The antivirus unit of Claim 39, wherein the antivirus unit and a first of said plurality of hosts have access to a same segment and access to said same segment by said first host is denied when said same segment is being accessed the antivirus unit.

59. (Previously Presented) The antivirus unit of Claim 39, wherein the antivirus unit and a first of said plurality of hosts have access to a same segment and the antivirus unit is allowed to perform virus scanning on said same segment while said same segment is being accessed by said first host.

60. (Previously Presented) The antivirus unit of Claim 39, wherein said means for accessing non-native files accesses a portion of said disk space using a logical disk unit, a cylinder number and a track number, and the antivirus unit further comprising:

means for performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed.